UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/729,209	12/05/2003	Jean-Pierre Duplessis.	MS306247.01/MSFTP552US	9483

27195 7590 05/31/2007

AMIN. TUROCY & CALVIN, LLP
24TH FLOOR, NATIONAL CITY CENTER
1900 EAST NINTH STREET
CLEVELAND, OH 44114

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	**PAPER NUMBER**
2136	

MAIL DATE	DELIVERY MODE
05/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/729,209	DUPLESSIS ET AL.	
	Examiner	Art Unit	
	Fatoumata Traore	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12,13,15-17,19,21 and 22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,12,13,15-17,19,21 and 22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on April 18, 2007 has been entered. Claims 1-10, 12, 13, 15-17, 19, 21, 22 are pending. Claims 11, 14, 18, and 20 are cancelled by the applicant and claims 1, 12, 13, 16, 19, 21, 22 are also amended by the applicant.

Claim Objections

2. Claims 11, 14 and 18 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant has canceled claims 11, 14, and 18, thus the objection has been withdrawn.

3. Claims 12, 13, 16 and 17 are objected to because of the following informalities: the examiner notes the use of acronyms (Wi-fi, EAPOL) throughout the claims without first including a description in plain text, as required. Applicant to address this objection has amended claims 9, 13, and 16. Therefore, the objection has been withdrawn.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1, 12, 21, 22 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the

invention. The "automatically" limitation if the detection component is waiting a predetermined amount of time for failures then the process is not exactly automatic. It is unclear to the examiner on how the applicant is achieving said limitation. Appropriated correction is required.

6. Clarification was given to application on the interpretation of claim 22 regarding the 112 6th paragraph during the telephonic interview conducted on March 15, 2007; therefore the rejection has been withdrawn.

Response to Amendment

7. Applicant's arguments with respect to claims 1-10, 12, 13, 15-17, 19, 21, 22 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1–3, 21, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Tsui** (US 2005/0063338) in view of **Muratov et al** (US 2003/0097596).

Claims 1, 21, and 22: **Tsui** discloses a seamless roaming apparatus, systems, and methods comprising:

i. A connection component that can connect a device to a plurality of wireless networks (to assist in providing high quality connection) (page 1, paragraph 0008); and;

ii. A detection component that automatically identifies an encryption type of an available wireless network, wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence (by detecting available network type) (page 1, paragraph 0008).

But **Tsui** does not explicitly disclose that the identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence. However **Muratov et al** discloses a system to protecting data within a portable electronic device, which further discloses that the type of the encryption is based on a failure of a portion of authentication (upon entry of a password (encryption) at 154, a determination is made at step 160 as whether the password is the valid password. If the password is valid, then the PDA is unlocked at step 162, and access to the data is allowed. If the password entered is not the valid password then at step 164 a determination is made as to whether a password entry limit has been set. If no limit is set, then another attempt at entering a password is

allowed at step 154. If the password entry limit has been set, then at step 166 a determination is made as to whether the limit has been exceeded) (page 6, paragraph 0104). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made o add a step of identifying the encryption type in **Tsui** 's disclosure. One would have been motivated to determine the encryption type in order to enter the corresponding key.

Claim 2: **Tsui** and **Muratov et al** disclose the seamless roaming system as in claim 1 above, and **Tsui** further discloses that the identification by the detection component is based, at least in part, upon receipt of an information element from a wireless network beacon. (A beacon detection circuit and software processing to detect the type of network that is available) (page 1, paragraph 0012).

Claim 3: **Tsui** and **Muratov et al** disclose the seamless roaming system as in claim 1 above, and **Tsui** further discloses that the wireless network comprise at least on of an unencrypted network, a wired equivalent Privacy (WEP) network requiring a WEP key, a Wi-Fi Protected Access (WPA) encrypted network requiring a WPA pre-shared key, an 802.1x-enabled network that does not support WPA, an 802.1x enabled network that does support WPA and a wireless provisioning services (WPS) support-enabled network (the wireless computing platform move from connecting to a first network to a second network) (page 1, paragraph 0009).

10. Claims 1, 4-10, 12, 13, 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Fascenda** (US 2004/0068653) in view of **Muratov et al** (US 2003/0097596).

Claim 1: **Fascenda** discloses a secure Wi-fi commutation system and method to enable automatic network roaming comprising:

iii. A connection component that can connect a device to a plurality of wireless networks (most access points have an integrated Ethernet controller to connect to an existing wired-Ethernet network) (page 1, paragraph 0006); and;

iv. A detection component that automatically identifies an encryption type of an available wireless network, wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence (Each network identifies itself using the beacon frame) (page 1, paragraph 0010).

But **Fascenda** does not explicitly disclose that the identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence. However **Muratov et al** discloses a system for protecting data within a portable electronic device, which further discloses that the type of the encryption is based

on a failure of a portion of authentication (upon entry of a password (encryption) at 154, a determination is made at step 160 as whether the password is the valid password. If the password is valid, then the PDA is unlocked at step 162, and access to the data is allowed. If the password entered is not the valid password then at step 164 a determination is made as to whether a password entry limit has been set. If no limit is set, then another attempt at entering a password is allowed at step 154. If the password entry limit has been set, then at step 166 a determination is made as to whether the limit has been exceeded) (page 6, paragraph 0104). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of identifying the encryption type in **Fascenda**'s disclosure. One would have been motivated to determine the encryption type in order to enter the corresponding key.

Claim 4: **Fascenda** and **Muratov et al** disclose a secure Wi-fi commutation system to enable automatic network roaming as in claim 1 above, and **Fascenda** further discloses that the identification by the detection component being based, at least in part, upon iterative probing of the available network (the client devices detects the presence of the network by listening for a probe request) (page 8, paragraph 069).

Claim 5: **Fascenda** and **Muratov et al** disclose a secure Wi-fi commutation system to enable automatic network roaming as in claim 4 above, and **Fascenda**

further discloses that the detection component attempts to connect to the wireless network as a wireless provisioning service-supporting network, the detection component determine that the network is a pre-shared key network if a failure in an authentication sequence from the wireless network beacon is determine (Even thought the secure mode enabled network appears to all potential users to be wide open , a user can connect to that network without having the proper respective network cryptographic keys. the authentication process discriminates between those users who have valid cryptographic keys and those who do not) (page 6, paragraph 0057).

Claim 6: **Fascenda** and **Muratov et al** disclose a secure Wi-Fi commutation system to enable automatic network roaming as in claim 5 above, and **Fascenda** further discloses that the detection component determining that the network as a Wi-Fi protected Access network if a failure in a particular piece of authentication (if the network is not secure mode enabled, the computing device attempts to connect to it using standard Wi-Fi parameters) (page 4, paragraph 0044).

Claim 7: **Fascenda** and **Muratov et al** disclose a secure Wi-fi commutation system to enable automatic network roaming as in claim 6 above, and **Fascenda** further discloses that a particular piece of authentication sequence comprise a type of length value sequence (Each authentication frame comprises an

authentication algorithm number preferably set to an integer number undefined in the 802.11 specification) (page 8, paragraph 0068).

Claim 8: **Fascenda** and **Muratov et al** discloses a secure Wi-fi commutation system to enable automatic network roaming as in claim 6 above, and **Fascenda** further identifies the type of the network if a particular piece of authentication sequence is received from the wireless network beacon (the beacon response frame comprises a Basic Service Set Identifier field that uniquely identifies the network and access point and distinguishes the current access point fro other access point) (page 8, paragraph 0069).

Claim 9: **Fascenda** and **Muratov et al** discloses a secure Wi-fi commutation system to enable automatic network roaming as in claim 1 above, and **Fascenda** further discloses that the detection component sends at least one of a connect message, an 802.1x EAPOL start message (a list of all Service Set Identifier currently available is displayed to the user, from which the user makes a choice which is also know as a passive mode (page 1, paragraph 0011).

Claim 10: **Fascenda** discloses a secure Wi-fi commutation system to enable automatic network roaming as in claim 1 above, and **Fascenda** further discloses that the detection component receives at least one of an associated message, an 802.1x identify request message, an authentication message and provisioning

message from a wireless network beacon (an alternative method of seeking wireless networks is know as active mode, whereby the Network Interface Card issues a probe request to cause all listening access points within range to respond with an identification frame containing their Service Set Identifier (page 1, paragraph 0011).

Claim 12: **Fascenda** discloses a secure Wi-fi commutation method to enable automatic network roaming comprising:

Attempting to connect to a wireless network as a wireless provisioning services supporting network (the computer device examines whether a Wi-Fi network exists and if found attempts to authenticate itself with the network) (Page4, paragraph 0044);

Determining whether the attempt was successful (if the network is enabled to operate in secure mode) (Page 4, paragraph 0044); and;

Prompting for a wired equivalent privacy key, if the attempt was not successful (if the network is not in secure mode enabled, the computing device attempts to connect using standard WI-Fi parameters) (Page1, paragraph 0044).

But **Fascenda** does not explicitly disclose that the identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence.

However **Muratov et al** discloses a system for protecting data within a portable electronic device, which further discloses that the type of the encryption is based

on a failure of a portion of authentication (upon entry of a password (encryption) at 154, a determination is made at step 160 as whether the password is the valid password. If the password is valid, then the PDA is unlocked at step 162, and access to the data is allowed. If the password entered is not the valid password then at step 164 a determination is made as to whether a password entry limit has been set. If no limit is set, then another attempt at entering a password is allowed at step 154. If the password entry limit has been set, then at step 166 a determination is made as to whether the limit has been exceeded) (page 6, paragraph 0104). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of identifying the encryption type in **Fascenda**'s disclosure. One would have been motivated to determine the encryption type in order to enter the corresponding key.

Claim 13: **Fascenda** and **Muratov et al** disclose a secure Wi-Fi communication method to enable automatic network roaming as in claim 12 above, and **Fascenda** further discloses a step of identifying the wireless network as a Wi-Fi Protected Access network, it the particular piece of authentication information has not been received (computing device examines whether a Wi-Fi exists and if found, attempts to authenticate itself with that network)(page 4, paragraph 0044) identifying the wireless network as a wireless provisioning services supporting network, if the particular piece of authentication information has been received (If the network is enabled to operate in secure, all of currently configured wireless

settings of the computing device are switched to secure mode and the login process is completely automated. If the network is not secure mode enabled, the computing device attempts to connect to it using standard Wi-Fi parameters) (page 4, paragraph 0044). But, **Fascenda** does not mention waiting up to a threshold period of time for a particular piece of authentication information that identifies a wireless provisioning services supporting network. However **Muratov et al** discloses a system for protecting data within a portable electronic device, which further discloses that the type of the encryption is based on a failure of a portion of authentication as discuss in claim 12 above (page 6, paragraph 0104). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of identifying the encryption type in **Fascenda** 's disclosure. One would have been motivated to determine the encryption type in order to enter the corresponding key.

Claim 19: **Fascenda** discloses a secure Wi-fi commutation system and method to enable automatic network roaming comprising: a data field comprising information identifying a type of wireless network connection based, at least in part, upon iterative probing of available network (the client devices detects the presence of the network by listening for a probe request) (page 8, paragraph 0069). But **Fascenda** does not explicitly disclose that the identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication

sequence. However **Muratov et al** discloses a system for protecting data within a portable electronic device, which further discloses that the type of the encryption is based on a failure of a portion of authentication (upon entry of a password (encryption) at 154, a determination is made at step 160 as whether the password is the valid password. If the password is valid, then the PDA is unlocked at step 162, and access to the data is allowed. If the password entered is not the valid password then at step 164 a determination is made as to whether a password entry limit has been set. If no limit is set, then another attempt at entering a password is allowed at step 154. If the password entry limit has been set, then at step 166 a determination is made as to whether the limit has been exceeded) (page 6, paragraph 0104). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of identifying the encryption type in **Fascenda**'s disclosure. One would have been motivated to determine the encryption type in order to enter the corresponding key.

11. Claims 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Fascenda** (US 2004/0068653) in view of **Balogh** (US 2001/0023446).

Claim 15: **Fascenda** discloses a secure Wi-fi commutation method to enable automatic network roaming comprising:

Determining whether a wireless network supports 802.1x (the wireless computing platform move from connecting to a first network to a second network) (page 1, paragraph 9), but **Fascenda** does not explicitly discloses:

> Identifying the wireless network as a wired equivalent privacy network requiring a wired equivalent privacy key, if the wireless network does not support 802.1x. Determining whether the wireless network supports wireless provisioning services, if the wireless network supports 802. ix; and, identifying the wireless network as an 802.1x network, if the wireless network does not supporting wireless provisioning services; and, Identifying the wireless network as a wireless provisioning services supporting network, if the wireless network supports wireless provisioning services.

However, **Balogh** discloses a method for accessing a network in a telecommunication system, which comprises:

> Determining whether a wireless network supports 802.1x (as a user of the MS wishes to originate a connection to a locally available network the WLAN functionality is activated) (page 4, paragraph 0034);
>
> Identifying the wireless network as a wired equivalent privacy network requiring a wired equivalent privacy key, if the wireless network does not support 802.1x.(in order to find out the information sets and networks that may be used in the current location area of the terminal MS, the MS performs a scanning of available networks) (page 4, paragraph 0034)

Determining whether the wireless network supports wireless provisioning services, if the wireless network supports 802.1x(scanning for access point AP1 as such is a basic functionality defined in IEEE 802.11standard, where the MS checks radio channels one by one by sending network identity request) (page 4, paragraph 0034); and,

Identifying the wireless network as an 802.1x network, if the wireless network does not supporting wireless provisioning services (and searching for network identity responses or (probe responses)) (page 4, paragraph 0034); and,

Identifying the wireless network as a wireless provisioning services supporting network, if the wireless network supports wireless provisioning services (probe responses comprising information of the access point. Preferably the probe responses comprises network names of sub-network SN1-3 the access points AP1-4 belong to) (page 4, paragraph 0034).

Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of identifying the wireless network type in **Fascenda**'s disclosure. One would have been motivated to determine the wireless network type in order to reduce the time spent by users in attempting to determine the type of such network

Claim 16: **Fascenda** and **Balogh** disclose a secure Wi-Fi communication method to enable automatic network roaming as in claim 15 above, **Fascenda** does not

mention distinguishing different type of network. However, **Balogh** discloses a similar method which further discloses a step of identifying (According to a preferred embodiment of the invention, the MS uses the scanned information of the networks to determine which information sets may be used 406. For instance, as the MS receives Probe responses 404, 405 from the AP1 and AP3, it compares 406 the network names in the Probe responses 404, 405 to the network names in the stored information sets and finds out that sub -network SN1 and SN2 are available. As the group of network names is advantageously specified (e.g. NW1LAN*), the network names (NW1LAN1, NW1LAN2) belonging to the same information set can be easily found. Further, the information set of the SN1 is then fully available, as the network names of the SN1 (NW1LAN1) and SN2 (NW1LAN2) are found. If there are more than one access point (AP1, AP2) in a single sub-network (SN1), the MS may receive the same network name many times in separate Probe responses. Thus the terminal MS can reliably determine the available networks and information sets, typically also the existing network names and identity requests may be used)(page4, paragraph 35). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of identifying the wireless network type in **Fascenda**'s disclosure. One would have been motivated to determine the wireless network type in order to reduce the time spent by users when attempting to connect to such network.

Claim 17: **Fascenda** and **Balogh** disclose a secure Wi-Fi communication method to enable automatic network roaming as in claim 16 above, **Fascenda** does not mention distinguishing different type of network. However, **Balogh** discloses a similar method which further discloses a step of identifying (According to a preferred embodiment of the invention, the MS uses the scanned information of the networks to determine which information sets may be used 406. For instance, as the MS receives Probe responses 404, 405 from the AP1 and AP3, it compares 406 the network names in the Probe responses 404, 405 to the network names in the stored information sets and finds out that sub -network SN1 and SN2 are available. As the group of network names is advantageously specified (e.g. NW1LAN*), the network names (NW1LAN1, NW1LAN2) belonging to the same information set can be easily found. Further, the information set of the SN1 is then fully available, as the network names of the SN1 (NW1LAN1) and SN2 (NW1LAN2) are found. If there are more than one access point (AP1, AP2) in a single sub-network (SN1), the MS may receive the same network name many times in separate Probe responses. Thus the terminal MS can reliably determine the available networks and information sets, typically also the existing network names and identity requests may be used)(page4, paragraph 35). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of identifying the wireless network type in **Fascenda**'s disclosure. One would have been motivated to determine

the wireless network type in order to reduce the time spent by users when attempting to connect to such network.

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:30 a.m. to 4:30 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar Moazzami, can be reached on (571) 272 4195. The fax phone

number for Formal or Official faxes to Technology Center 2100 is (571) 273-3800. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 274-1685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
January 3, 2007

James W. Myhre
Supervisory Patent Examiner